IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: John BORDER *et al.*	Confirmation No.: 1446
Filed: September 14, 2000	Group Art Unit: 2157
Attorney Docket: PD-200053	Examiner: El Chanti, Hussein

For: **PERFORMANCE ENHANCING PROXY AND METHOD FOR ENHANCING PERFORMANCE**

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated December 24, 2008.

I. REAL PARTY IN INTEREST

The real party in interest is HUGHES ELECTRONICS CORPORATION.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III. STATUS OF THE CLAIMS

Claims 3, 5-9, 11-29, 32, 34-38, and 40-59 are pending in this appeal, in which claims 1, 2, 4, 10, 30, 31, 33, 39, and 60 are canceled; and claims 61 and 62 have been withdrawn in accordance with a restriction requirement. No claim is allowed. This appeal is therefore taken from the final rejection of claims 3, 5-9, 11-29, 32, 34-38, and 40-59 on July 29, 2008.

IV. STATUS OF AMENDMENTS

All amendments have been entered. The appealed claims are as shown in the Appendix attached hereto.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention addresses problems associated with improving performance of protocols on network paths, particularly the performance of the TCP/IP protocol on the Internet.

Independent claim 3 provides for the following:

3. A network apparatus, comprising:

a proxy (See, e.g., Specification, page 7, line 22-page 8, line 9; Fig. 4, element 200) which facilitates communication with other network entities (See, e.g., Specification, page 6, lines 9-24; hosts 110, 150 in Fig. 3) by performing at least one performance enhancing function (See, e.g., Specification, page 6, line 23-page 7, line 19), the proxy communicating with the other network entities via a first type of connection (See, e.g., Specification, page 6, line 13; Fig. 3, TCP connections) and a second type of connection (See, e.g., Specification, page 6, lines 13-15;

Fig. 3, Backbone connection), wherein the proxy establishes multiple connections of the first type associated with different applications (See, e.g., Specification, page 14, lines 21-23), and includes

a spoofing element (See, e.g., Specification, page 8, lines 4-5; Fig. 4, TSK element 280) configured to intercept and alter a data flow within one of the connections to add to or delete from the data flow to reduce startup latency (See, e.g., Specification, page 8, line 9-page 9, line 9), the spoofing element only spoofing connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired (See, e.g., Specification, page 10, line 24-page 13, line 13, especially page 11, lines 1-6; Figs. 5 and 6), and

a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type (See, e.g., Specification, page 14, line 20-page 15, line 19).

Dependent claim 7 provides for the following:

7. The network apparatus of claim 6, wherein said spoofing element defines the at least one spoofing rule in a spoofing profile (See, e.g., Specification, page 12, lines 16-30).

Dependent claim 13 provides for the following:

13. The network apparatus of claim 12, wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile (See, e.g., Specification, page 17, lines 10-23).

Independent claim 32 provides for the following:

32. A method for providing data communication with a plurality of network entities (See, e.g., Specification, page 6, lines 9-24; hosts 110, 150 in Fig. 3), comprising:

facilitating communication with the network entities (See, e.g., Specification, page 6, lines 9-24; hosts 110, 150 in Fig. 3) by performing at least one performance enhancing function (See, e.g., Specification, page 6, line 23-page 7, line 19);

communicating with the network entities via a first type of connection and a second type of connection (See, e.g., Specification, page 6, line 13; Fig. 3, TCP connections as the first type, and page 6, lines 13-15; Fig. 3, Backbone connection as the second type);

establishing multiple connections of the first type associated with different applications (See, e.g., Specification, page 14, lines 21-23);

intercepting and altering a data flow within one of the connections to add to or delete from the data flow to reduce startup latency (See, e.g., Specification, page 8, line 9-page 9, line 9);

spoofing only connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired (See, e.g., Specification, page 10, line 24-page 13, line 13, especially page 11, lines 1-6; Figs. 5 and 6); and

selectively multiplexing the spoofed connections onto a single connection of the second type (See, e.g., Specification, page 14, line 20-page 15, line 19).

Dependent claim 36 provides for the following:

36. The method of claim 35, wherein said spoofing step defines the at least one spoofing rule in a spoofing profile (See, e.g., Specification, page 12, lines 16-30).

Dependent claim 42 provides for the following:

42. The network apparatus of claim 41, wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile (See, e.g., Specification, page 17, lines 10-23).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 3, 5-9, 11-29, 32, 34-38, and 40-59 are anticipated under 35 U.S.C § 102(e) by *Yates et al.* (US 6,167,438)?

VII. ARGUMENT

A. CLAIMS 3, 5-9, 11-29, 32, 34-38, AND 40-59 ARE NOT ANTICIPATED OVER *YATES ET AL.*, BECAUSE *YATES ET AL.* FAILS TO DISCLOSE SELECTIVELY MULTIPLEXING SPOOFED CONNECTIONS ONTO A SINGLE CONNECTION OF THE SECOND TYPE.

To anticipate a patent claim, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383, 58 USPQ2d 1286, 1291 (Fed. Cir. 2001); *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

Independent claim 3 recites, *inter alia*, "a **multiplexing element** configured to **selectively multiplex** the spoofed connections onto **a single connection of the second type**." Independent claim 32 recites, *inter alia*, "**selectively multiplexing** the spoofed connections onto **a single connection of the second type**." These features are not disclosed in *Yates et al.*

The Examiner, in the Final Office Action, contends that such features are taught in *Yates et al.* at col. 9, line 54-col. 10, line 15. This portion of *Yates et al.* provides as follows:

> To overcome this hurdle, in the preferred embodiment, intermediate routers 14 have some awareness of the TCP protocol. TCP aware routers 14 are able to detect TCP connection requests to all HTTP servers (i.e., a {SYN} packet directed to the HTTP port), and have the ability to act as a proxy for, or "spoof" the home server 20.
>
> This functionality is implemented by the snooper 28. In particular, snoopers 28 located in routers 14 on the path to a home server 20 inspect packets that fly-by, identify such packets, and intercept any {SYN} packets directed to HTTP home servers 20. As {SYN} packets do not contain any information identifying which document the client 12 intends to request, the snooper 28 acts as a proxy for, or "spoofs" the home server 20, by establishing a connection between the client 12 and the local transport layer in the cache server 16, and noting the initial sequence numbers used by both the client 12 and the local transport layer.
>
> After the connection is established the snooper 28 inspects all packets that fly-by, and waits for the corresponding {GET} request. Once the {GET} request arrives the snooper 28 queries the local filter 26 and the resource manager 24 to determine if the requested document is cached. If the document is cached the snooper 28 forwards the HTTP {GET} message to the local resource manager 24, waits for the resource manager 24 to service the request, and then terminates the connection. Otherwise, the requested document is not cached (i.e., the filter 26 or resource manager 24 missed). Several different approaches may be taken to servicing the document request at this point.

As is clear from this passage of *Yates et al.*, and the remainder of the reference, there is no multiplexing operation, particularly in the manner claimed, disclosed. While the cited passage indicates that multiple TCP/IP connections may be established with home server 20, neither the home server nor any other element within *Yates et al.*, multiplexes these connections.

At page 8 of the Final Office Action, the Examiner equates the plurality of TCP connection requests received by the router in *Yates et al.* to the claimed connections of the "first type" and equates the connection between the client and the local transport layer established by

the home server as the claimed "second type" of connection. Respectfully, this rationale is flawed.

Appellants do not gainsay that TCP connections in *Yates et al.* may be interpreted as a "first type" of connection. However, in accordance with the language of claims 3 and 32, there must be "a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type" and "selectively multiplexing the spoofed connections onto a single connection of the second type," respectively. The snooper 28 of *Yates et al.* provides no multiplexing function. Rather, the snoopers 28 are located in the routers 14 on the path to the home server 20 and the snoopers inspect packets that fly-by, identify those packets and intercept certain packets, viz., those packets that do not identify a document the client intends to request. The snooper acts as a proxy for the home server by establishing a connection between the client and the local transport layer in a cache server 16. It is only **after** this connection is established that the snooper inspects all packets that fly-by, waiting for a corresponding request to retrieve a document. However, this "spoofed" connection between the client and the local transport layer in the cache server is not "multiplexed" and clearly is not "multiplexed…onto a single connection of the second type."

Moreover, Appellants note that independent claims 3 ("the spoofing element only **spoofing connections of the first type**…") and 32 ("spoofing **only connections of the first type**…") recite that the "spoofing connections" are connections of the "first type." The Examiner, on the other hand, has identified the connection between the client and the local transport layer as the "second type" of connection, but the connection between the client and the local transport layer is the "spoofed" connection, as indicated at col. 9, line 66-col. 10, line 2 of *Yates et al.* Thus, the Examiner's rationale would result in spoofing connections of the "second

type," rather than the "first type," being multiplexed (even if there was a teaching of multiplexing in *Yates et al*., which there is not), contrary to the instant claim language.

Because *Yates et al.* contains absolutely no teaching of "multiplexing" (let alone a teaching of "a **multiplexing element** configured to **selectively multiplex** the spoofed connections onto **a single connection of the second type**" or "**selectively multiplexing** the spoofed connections onto **a single connection of the second type**," and the Examiner has failed to specifically identify any such "multiplexing" operation in the reference, no *prima facie* case of anticipation has been established.

B. CLAIMS 7, 13, 36, AND 42 ARE NOT ANTICIPATED OVER *YATES ET AL.*, BECAUSE *YATES ET AL.* FAILS TO DISCLOSE THE DEFINING OF A SPOOFING RULE IN A SPOOFING PROFILE OR THE DEFINING OF A PRIORITIZING RULE IN A PRIORITIZING PROFILE.

Claims 7, 13, 36, and 42 are separately patentable because these claims further recite the defining of a spoofing profile and a prioritizing profile, features that are undisclosed *Yates et al.*

The Examiner cites col. 9, line 60-col. 10, line 30 for a disclosure of these profiles, adding the citation of col. 14, line 35-col. 16, line 60, specifically regarding a "prioritizing profile."

The spoofing "rule" in col. 9, line 60-col. 10, line 30, to the extent there is one, is directed to the snooper 28 spoofing a home server by establishing a connection between the client 12 and the local transport layer in the cache server 16. Thus, no "spoofing rule" is established in *Yates et al.*, other than the mere connection of the client to the local transport layer. Thus, there is no "spoofing **profile**" disclosed in *Yates et al.* and there is none necessary because *Yates et al.* discloses no set of "rules" that may be applied in accordance with certain criteria, as, for example, disclosed on page 12 of the instant specification. Thus, the features of instant claims 7 and 36 are not disclosed by *Yates et al.*

Further, there is no "prioritizing profile" in *Yates et al.*, as specified in instant claims 13 and 42. While *Yates et al.* indicates at col. 14, lines 36 *et seq.* that certain objectives include extracting the "maximum capacity" of cache servers and reducing "response time," are desired, thus suggesting a certain priority of operations, there is no disclosure of a "prioritizing **profile**" in *Yates et al.* because there is no set of "rules" disclosed therein that may be applied in accordance with certain criteria, as for example, disclosed on page 17 of the instant specification.

The rejection of claims 3, 5-9, 11-29, 32, 34-38, and 40-59 under 35 U.S.C § 102(e) must be reversed, because *Yates et al.* does not disclose each and every limitation of the claims.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

February 2, 2009
Date

/Phouphanomketh Ditthavong/
Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

Errol A. Krass
Attorney/Agent for Applicant(s)
Reg. No. 60090

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax.703-519-9958

CLAIMS APPENDIX

3. A network apparatus, comprising:

a proxy which facilitates communication with other network entities by performing at least one performance enhancing function, the proxy communicating with the other network entities via a first type of connection and a second type of connection, wherein the proxy establishes multiple connections of the first type associated with different applications, and includes

a spoofing element configured to intercept and alter a data flow within one of the connections to add to or delete from the data flow to reduce startup latency, the spoofing element only spoofing connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired , and

a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type.

5. The network apparatus of claim 3, wherein said spoofing element assigns spoofing resources, including buffer space and control blocks, to the spoofed connections.

6. The network apparatus of claim 3, wherein said spoofing element spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

7. The network apparatus of claim 6, wherein said spoofing element defines the at least one spoofing rule in a spoofing profile.

8. The network apparatus of claim 3, wherein the spoofing element spoofs acknowledgements (ACKs).

9. The network apparatus of claim 3, wherein the spoofing element spoofs a three-way handshake between said network apparatus and another network entity.

11. The network apparatus of claim 3, wherein the proxy includes a prioritization element, which prioritizes connections of the first type to determine what priority level of the connection of the second type, each of the connections of the first type are assigned.

12. The network apparatus of claim 11, wherein said prioritizing element prioritizes connections using at least one prioritizing rule based on destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field, a type of data contained within the connection or combinations thereof.

13. The network apparatus of claim 12, wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile.

14. The network apparatus of claim 3, wherein the proxy includes a path selection element, which selects a path for data associated with connections of the first type across connections of the second type or connections of other types.

15. The network apparatus of claim 14, wherein said path selection element can select up to N paths (N>1), where the Nth path is selected only if the (N-1)th path fails.

16. The network apparatus of claim 15, wherein said path selection element selects a path using at least one path selection rule based on priority, a destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field or combinations thereof.

17. The network apparatus of claim 16, wherein said path selection element defines the at least one path selection rule in a path selection profile.

18. The network apparatus of claim 3, wherein the proxy includes a compression and encryption element, which compresses and encrypts data associated with connections of the first type for transmission across connections of the second type.

19. The network apparatus of claim 3, wherein the first connection uses a high layer protocol.

20. The network apparatus of claim 3, wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

21. The network apparatus of claim 3, wherein the second connection is a backbone connection.

22. The network apparatus of claim 3, wherein the backbone connection is via a wireless link.

23. The network apparatus of claim 22, wherein the wireless link has high latency and high error rate.

24. The network apparatus of claim 22, wherein the wireless link is a satellite link.

25. The network apparatus of claim 3, wherein said network apparatus is a component of a network gateway.

26. The network apparatus of claim 3, wherein said network apparatus is a component of a host.

27. The network apparatus of claim 3, wherein said network apparatus is a component of a hub.

28. The network apparatus of claim 3, wherein said network apparatus is a component of a VSAT.

29. The network apparatus of claim 3, wherein said network apparatus is a component of a router.

32. A method for providing data communication with a plurality of network entities, comprising:

facilitating communication with the network entities by performing at least one performance enhancing function;

communicating with the network entities via a first type of connection and a second type of connection;

establishing multiple connections of the first type associated with different applications;

intercepting and altering a data flow within one of the connections to add to or delete from the data flow to reduce startup latency;

spoofing only connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired ; and

selectively multiplexing the spoofed connections onto a single connection of the second type.

34. The method of claim 32, wherein said spoofing step assigns spoofing resources, including buffer space and control blocks, to the spoofed connections.

35. The method of claim 32, wherein said spoofing step spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

36. The method of claim 35, wherein said spoofing step defines the at least one spoofing rule in a spoofing profile.

37. The method of claim 32, further comprising:

spoofing acknowledgements (ACKs).

38. The method of claim 32, further comprising:

spoofing a three-way handshake another network entity.

40. The method of claim 32, further comprising:

prioritizing connections of the first type to determine what priority level of the connection of the second type, each of the connections of the first type are assigned.

41. The method of claim 40, wherein said prioritizing step prioritizes connections using at least one priority rule based on destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field, type of data contained within the connection or combinations thereof.

42. The network apparatus of claim 41, wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile.

43. The method of claim 32, further comprising:

selecting a path for data associated with connections of the first type across connections of the second type or connections of other types.

44. The method of claim 43, wherein said selection step selects up to N paths (N>1), where the Nth path is selected only if the (N-1)th path fails.

45. The method of claim 44, wherein said selection step selects a path using at least one path selection rule based on priority, a destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field or combinations thereof.

46. The method of claim 45, wherein said selection step defines the at least one path selection rule in a path selection profile.

47. The method of claim 32, further comprising:
compressing and encrypting data associated with connections of the first type for transmission across connections of the second type.

48. The method of claim 32, wherein the first connection uses a high layer protocol.

49. The method of claim 32, wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

50. The method of claim 32, wherein the second connection is a backbone connection.

51. The method of claim 50, wherein the backbone connection is via a wireless link.

52. The method of claim 32, wherein the wireless link has high latency and high error rate.

53. The method of claim 32, wherein the wireless link is a satellite link.

54. The method of claim 32, wherein said method is performed in a network gateway.

55. The method of claim 32, wherein said method is performed in a host.

56. The method of claim 32, wherein said method is performed in a hub.

57. The method of claim 32, wherein said method is performed in a VSAT.

58. The method of claim 32, wherein said method is performed in a router.

59. The method of claim 32, wherein said method is performed in a switch.

X. EVIDENCE APPENDIX

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI. RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.